

# Managing The Insider Threat: What Every Organization Should Know

8.8.13 • 9:00 AM ET-5:00 PM ET



## Overview of the Threat Posed by Insiders to Critical Assets



**Randy Trzeciak**

Technical Manager - CERT Enterprise Threat and Vulnerability Management Team & CERT Insider Threat Center

Randy is Technical Manager of CERT's Enterprise Threat and Vulnerability Management Team and the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The team's mission is to assist organizations in improving their security posture and incident response capability by researching technical threat areas, developing and conducting information security assessments, and providing information, solutions and training for preventing, detecting, and responding to illicit activity.



**David Mundie**

CERT CSIRT Development Team Member

David Mundie is a member of the CSIRT Development Team within the CERT® Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. He has been at CERT since 2000 and has worked in a variety of areas including insider threat, malware analysis, and incident management capability metrics. From 2006 to 2009, he was a member of the Q-CERT project, which established a national information security team for the country of Qatar.



**Software Engineering Institute**

**Carnegie Mellon**

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsidethreat](#)  
© 2013 Carnegie Mellon University

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>08 AUG 2013</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2013 to 00-00-2013</b>	
4. TITLE AND SUBTITLE <b>Overview of the Threat Posed by Insiders to Critical Assets</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>47</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

# What is the CERT Insider Threat Center?

Center of insider threat expertise



Began working in this area in 2001 with the U.S. Secret Service

Our mission: *The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.*

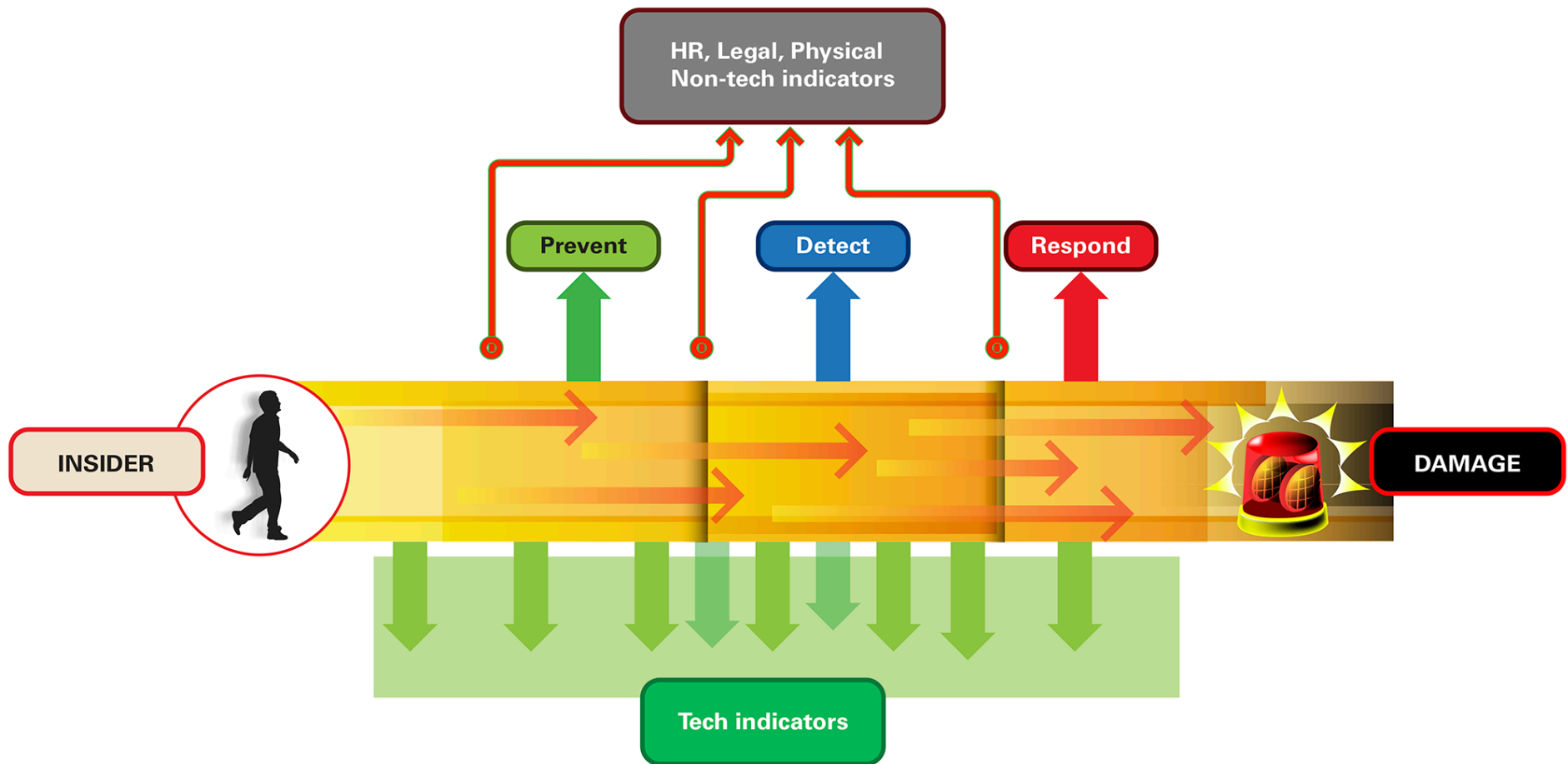


Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsidethreat](#)  
© 2013 Carnegie Mellon University

# Goal for an Insider Threat Program



*Opportunities for prevention, detection, and response for an insider incident*



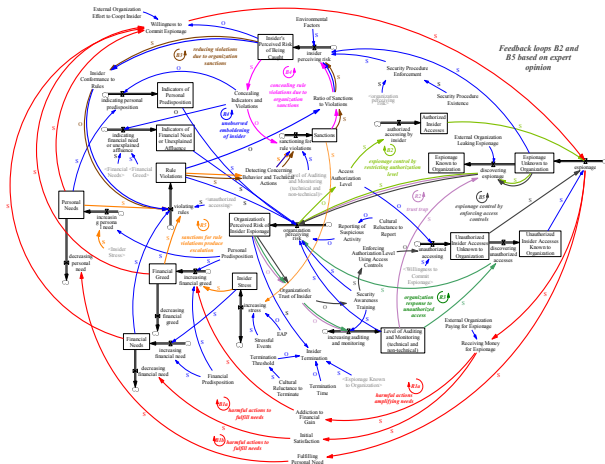
Software Engineering Institute

Carnegie Mellon

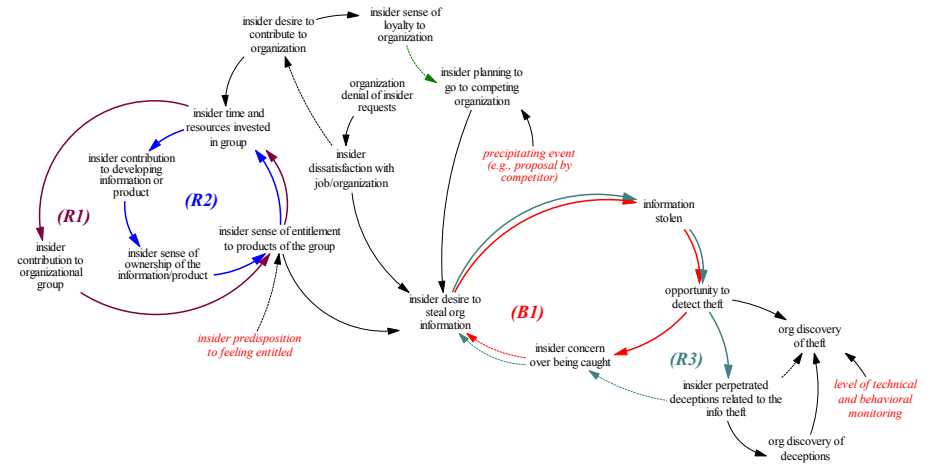
Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# CERT's Unique Approach to the Problem

# Research Models



## Deriving Candidate Controls and Indicators



*Our lab transforms that into this...*

Splunk Query Name: Last 30 Days - Possible Theft of IP

```
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *" | eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name "@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address, recipient_address, message subject, total bytes'
```

# The Insider Threat

There is not one “type” of insider threat

- Threat is to an organization’s critical assets
  - People
  - Information
  - Technology
  - Facilities
- Based on the motive(s) of the insider
- Impact is to Confidentiality, Availability, Integrity

There is not one solution for addressing the insider threat

- Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

## Separate the “Target” from the “Impact” from the “Actor”

Target	Impact	Actor(s)
<b>Critical Assets</b> <ul style="list-style-type: none"><li>• People</li><li>• Technology</li><li>• Information</li><li>• Facilities</li></ul>	<b>Confidentiality</b> <b>Availability</b> <b>Integrity</b>	<b>Employees</b> <ul style="list-style-type: none"><li>• Current</li><li>• Former</li></ul> <b>Contractors</b> <b>Subcontractors</b> <b>Suppliers</b> <b>Trusted Business Partners</b>
WHAT	HOW	WHO



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# What is a Malicious Insider Threat?

*Current or former employee, contractor, or other business partner who*

- *has or had authorized access to an organization's network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.*





# What is an Unintentional Insider Threat?

*Current or former employee, contractor, or other business partner who*

- *who has or had authorized access to an organization's network, system, or data and who, through*
- *their action/inaction without malicious intent*
- *cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.*



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](https://twitter.com/CERTinsiderthreat)  
© 2013 Carnegie Mellon University

# Types of Insider Crimes

## ***Insider IT sabotage***

An insider's use of IT to direct specific harm at an organization or an individual.

## ***Insider theft of intellectual property (IP)***

An insider's use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.

## ***Insider fraud***

An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud (identity theft, credit card fraud).

## ***National Security Espionage***

The act of stealing and delivering, or attempting to deliver, information pertaining to the national defense of the United States to agents or subjects of foreign countries, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation.



**Software Engineering Institute**

**Carnegie Mellon**

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University



# Insider Crime Profiles



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsidethreat](#)  
© 2013 Carnegie Mellon University

# IT Sabotage



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# TRUE STORY:

**SCADA systems for an oil-exploration company is temporarily disabled...**

***A contractor, who's request for permanent employment was rejected, planted malicious code following termination***



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# Other Cases of IT Sabotage

Financial Institution customers lose all access to their money from Friday night through Monday

- Fired system administrator sabotages systems on his way out

A subcontractor at an energy management facility breaks the glass enclosing the emergency power button, then shuts down computers that regulate the exchange of electricity between power grids, even though his own employer had disabled his access to their own facility following a dispute.

- Impact: Internal power outage; Shutdown of electricity between the power grids in the US.

Former employee of auto dealer modified vehicle control system after being laid off

- Searched for known customers and sent out unwarranted signals to vehicle control devices disabled ignitions and set off alarms

A security guard at a U.S. hospital, after submitting resignation notice, obtained physical access to computer rooms

- Installed malicious code on hospital computers, accessed patient medical records



**Software Engineering Institute**

**CarnegieMellon**

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# Summary of Insider Threats

	IT Sabotage
Current or former employee?	Former
Type of position	Technical (e.g. sys admins, programmers, or DBAs)
Gender	Male
Target	Network, systems, or data
Access used	Unauthorized
When	Outside normal working hours
Where	Remote access



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University



# Fraud



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University



## TRUE STORY:

An undercover agent who claims to be on the “No Fly list” buys fake drivers license from a ring of DMV employees...

*The 7 person identity theft ring consisted of 7 employees who sold more than 200 fake licenses for more than \$1 Million.*



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsidethreat](#)  
© 2013 Carnegie Mellon University

# Other Cases of Fraud

An accounts payable clerk, over a period of 3 years, issued 127 unauthorized checks to herself and others...

- Checks totaled over \$875,000

A front desk office coordinator stole PII from hospital...

- Over 1100 victims and over \$2.8 M in fraudulent claims

A database administrator at major US Insurance Co. downloaded 60,000 employee records onto removable and solicited bids for sale over the Internet

An office manager for a trucking firm fraudulently puts her husband on the payroll for weekly payouts, and erases records of payments...

- Over almost a year loss of over \$100K



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# Summary of Insider Threats

	IT Sabotage	Fraud
<b>Current or former employee?</b>	Former	Current
<b>Type of position</b>	Technical (e.g. sys admins, programmers, or DBAs)	Non-technical (e.g. data entry, customer service) or their managers
<b>Gender</b>	Male	Fairly equally split between male and female
<b>Target</b>	Network, systems, or data	PII or Customer Information
<b>Access used</b>	Unauthorized	Authorized
<b>When</b>	Outside normal working hours	During normal working hours
<b>Where</b>	Remote access	At work



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# Theft of Intellectual Property



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# TRUE STORY:

Research scientist downloads 38,000 documents containing his company's trade secrets before going to work for a competitor...

*Information was valued at  
\$400 Million*



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsidert threat](#)  
© 2013 Carnegie Mellon University

# Other Cases of Theft of IP

A technical operations associate at a pharmaceutical company downloads 65 GB of information, including 1300 confidential and proprietary documents, intending to start a competing company, in a foreign country...

- Organization spent over \$500M in development costs

Simulation software for the reactor control room in a US nuclear power plant was being run from outside the US...

- A former software engineer born in that country took it with him when he left the company.



Software Engineering Institute

CarnegieMellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University



# Summary of Insider Threats

	IT Sabotage	Fraud	Theft of Intellectual Property
<b>Current or former employee?</b>	Former	Current	Current (within 30 days of resignation)
<b>Type of position</b>	Technical (e.g. sys admins, programmers, or DBAs)	Non-technical (e.g. data entry, customer service) or their managers	Technical (e.g. scientists, programmers, engineers) or sales
<b>Gender</b>	Male	Fairly equally split between male and female	Male
<b>Target</b>	Network, systems, or data	PII or Customer Information	IP (trade secrets) –or customer Info
<b>Access used</b>	Unauthorized	Authorized	Authorized
<b>When</b>	Outside normal working hours	During normal working hours	During normal working hours
<b>Where</b>	Remote access	At work	At work



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University



# Ontologies for Insider Threat Research



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsidethreat](#)  
© 2013 Carnegie Mellon University



# Vision

---

The most important attributes would be the construction of a common language and a set of basic concepts about which the security community can develop a shared understanding... a common language and agreed-upon experimental protocols will facilitate the testing of hypotheses and validation of concepts. –Jason Report



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsidethreat](#)  
© 2013 Carnegie Mellon University

# Medical Ontologies

**OLSVis** Gene Ontology (GO)

• roots  
+ filters

**mitochondrion** (GO:0005739)

A semiautonomous, self replicating organelle that occurs in varying numbers, shapes, and sizes in the cytoplasm of virtually all eukaryotic cells. It is notably the site of tissue respiration.

exact synonym:	mitochondria
subset goslim aspergillus:	Aspergillus GO slim
subset goslim candida:	Candida GO slim
subset goslim generic:	Generic GO slim
subset goslim metagenomics:	Metagenomics GO slim
subset goslim pir:	PIR GO slim
subset goslim plant:	Plant GO slim
subset goslim yeast:	Yeast GO slim
xref definition:	ISBN:0198506732
xref analog:	NIF_Subcellular:sao1860313010
xref analog:	Wikipedia:Mitochondrion

Child terms:

- mitochondrial derivative
- mitochondrial part
- Nebenkern

```
graph TD
    cell -- part --> cellular_component
    cell -- is --> intracellular
    cell -- is --> cytoplasm
    cellular_component -- is --> intracellular
    cellular_component -- is --> cytoplasm
    cytoplasm -- part --> intracellular
    cytoplasm -- is --> cytoplasmic_part[cytoplasmic part]
    cytoplasm -- is --> mitochondrion
    intracellular -- part --> intracellular_part[intracellular part]
    intracellular -- is --> organelle
    intracellular -- is --> intracellular_organelle[intracellular organelle]
    intracellular_part -- is --> organelle
    intracellular_part -- is --> intracellular_organelle
    organelle -- is --> intracellular_organelle
    organelle -- is --> membrane_bounded_organelle[membrane-bounded organelle]
    intracellular_organelle -- is --> membrane_bounded_organelle
    mitochondrion -- is --> mitochondrial_derivative[mitochondrial derivative]
    mitochondrion -- is --> mitochondrial_part[mitochondrial part]
    Nebenkern -- is --> mitochondrion
```

# Google Knowledge Graph


Google

[Web](#) [Images](#) [Maps](#) [Shopping](#) [News](#) [More](#) [Search tools](#)

About 44,300,000 results (0.27 seconds)

[Leonardo da Vinci - Wikipedia, the free encyclopedia](#)  
[en.wikipedia.org/wiki/Leonardo\\_da\\_Vinci](http://en.wikipedia.org/wiki/Leonardo_da_Vinci)  
**Leonardo di ser Piero da Vinci** (April 15, 1452 – May 2, 1519, Old Style) was an Italian Renaissance polymath: painter, sculptor, architect, musician, ...  
[Personal life](#) - [List of works](#) - [Science and inventions](#) - [Mona Lisa](#)

[Leonardo da Vinci - Museum of Science](#)  
[www.mos.org/leonardo/](http://www.mos.org/leonardo/)  
Provides a biography along with a multimedia section including images of his works.

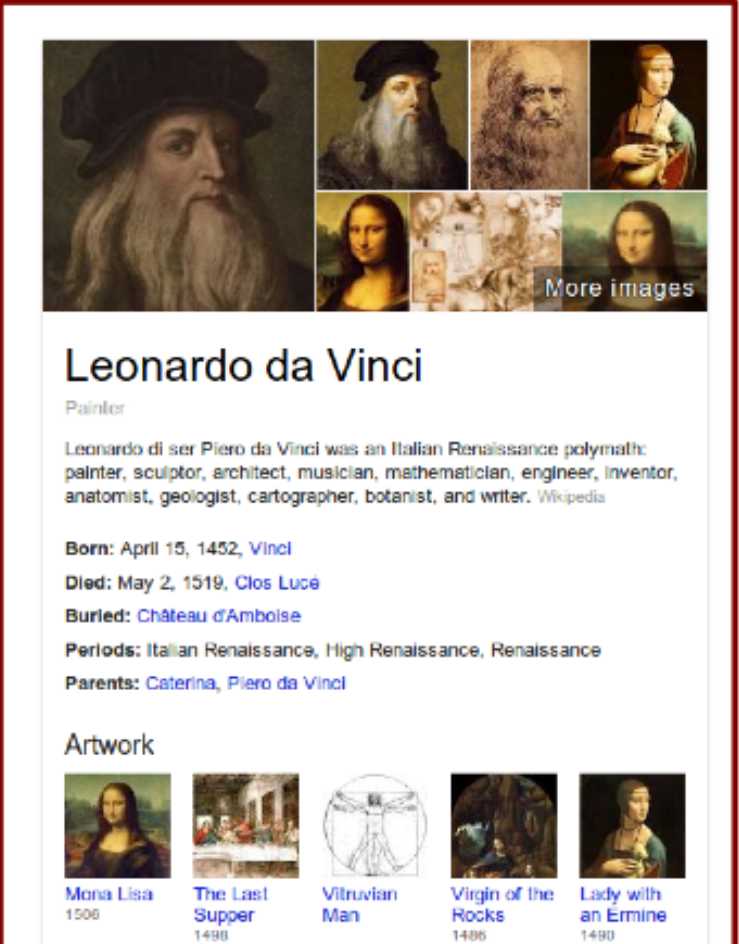
[Leonardo da Vinci Biography - Facts, Birthday, Life Story ...](#)  
[www.biography.com](http://www.biography.com) > People  
Sep 28, 2011  
A leading figure of the Italian Renaissance, **Leonardo da Vinci's** work has epitomized beauty for generations ...  
 [More videos for leonardo da vinci »](#)

[Leonardo da Vinci](#)  
[www.ucmp.berkeley.edu/history/vinci.html](http://www.ucmp.berkeley.edu/history/vinci.html)  
Sometimes supernaturally, marvelously, they all congregate in one individual. . . . This was seen and acknowledged by all men in the case of **Leonardo da Vinci** ...

[Leonardo da Vinci Paintings, Drawings, Quotes, Inventions, Biography](#)  
[www.leonardodavinci.net/](http://www.leonardodavinci.net/)  
**Leonardo da Vinci** was born on 15 April 1452 in the town of **Vinci**, the illegitimate son of the notary Ser Piero **da Vinci** and a peasant woman called Caterina.

[Leonardo Da Vinci - The complete works](#)  
[www.leonardoda-vinci.org/](http://www.leonardoda-vinci.org/)  
**Leonardo Da Vinci** - Homepage. The complete works, large resolution images, ecard, rating, slideshow and more! One of the largest **Leonardo Da Vinci** ...

[Leonardo da Vinci — History.com Articles, Video, Pictures and Facts](#)








**Leonardo da Vinci**  
Painter

Leonardo di ser Piero da Vinci was an Italian Renaissance polymath: painter, sculptor, architect, musician, mathematician, engineer, inventor, anatomist, geologist, cartographer, botanist, and writer. [Wikipedia](#)

**Born:** April 15, 1452, [Vinci](#)  
**Died:** May 2, 1519, [Clos Lucé](#)  
**Buried:** [Château d'Amboise](#)  
**Periods:** Italian Renaissance, High Renaissance, Renaissance  
**Parents:** [Caterina](#), [Piero da Vinci](#)

**Artwork**

 <a href="#">Mona Lisa</a> 1506	 <a href="#">The Last Supper</a> 1498	 <a href="#">Vitruvian Man</a>	 <a href="#">Virgin of the Rocks</a> 1486	 <a href="#">Lady with an Ermine</a> 1490
--	--	--	--	--



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
[Twitter #CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# Google Knowledge Graph (cont.)

- Huge “semantic network” of over 570 million objects and 18 billion facts (500 million objects and 3.5 billion facts)
- Sources: CIA World Factbook, Wikipedia, **Freebase**
- Facts about: people, actors, directors, movies, cities, countries, recipes, etc.
- Available in multiple languages; localized search results

<http://googleblog.blogspot.co.uk/2012/05/introducing-knowledge-graph-things-not.html>

<http://www.newyorker.com/online/blogs/culture/2012/05/google-knowledge-graph.html>

<http://venturebeat.com/2013/01/22/larry-page-on-googles-knowledge-graph-were-still-at-1-of-where-we-want-to-be/>

[http://news.cnet.com/8301-1023\\_3-57435114-93/google-bringing-new-smarts-to-search-with-knowledge-graph/](http://news.cnet.com/8301-1023_3-57435114-93/google-bringing-new-smarts-to-search-with-knowledge-graph/)

12



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter **#CERTinsiderthreat**  
© 2013 Carnegie Mellon University

# Ontology Work at CERT

## Incident Management

- Incident Management Body of Knowledge
- MAL: Ontology-based Competency Model

## General

- 10-step methodology for developing ontologies
  - Terms, controlled vocabulary, static relationships, dynamic relationships

## Insider Threat

- Lexicographic insider threat ontology
- Trust ontology
- Indicator ontology
- Unintentional insider threat ontology



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# A Lexicographic Ontology of Insider Threat

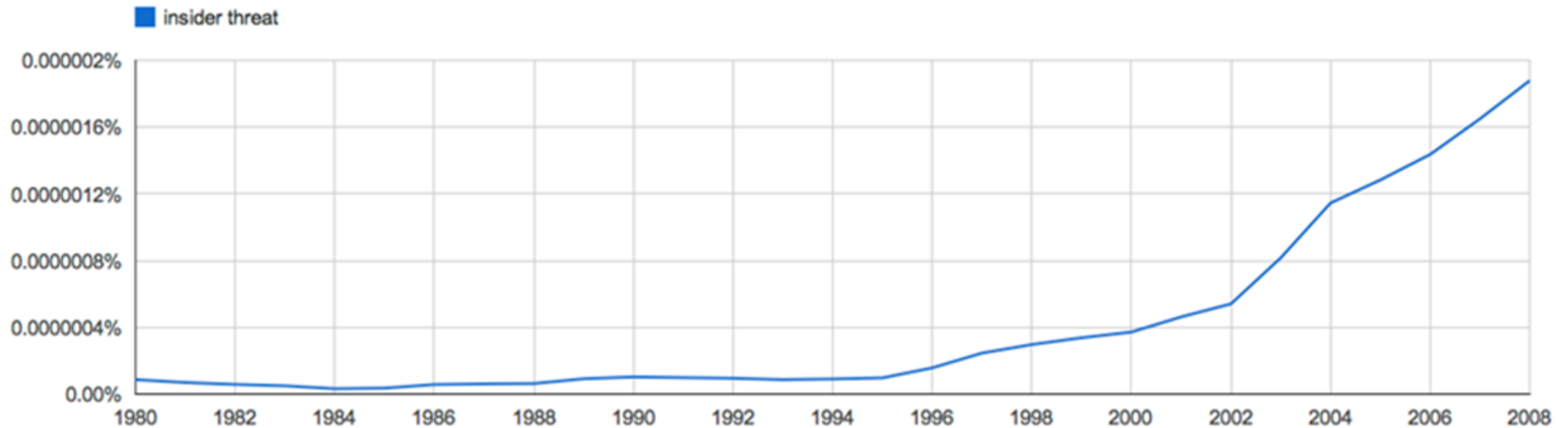


Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# From Lexicography to Ontology



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# 42 Definitions

- Encountered during a literature search
- Two example definitions
  - *is someone who is authorized to use computers and networks*
  - *is anyone who operated inside the security perimeter*



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University



# From Natural Language to Formal Language

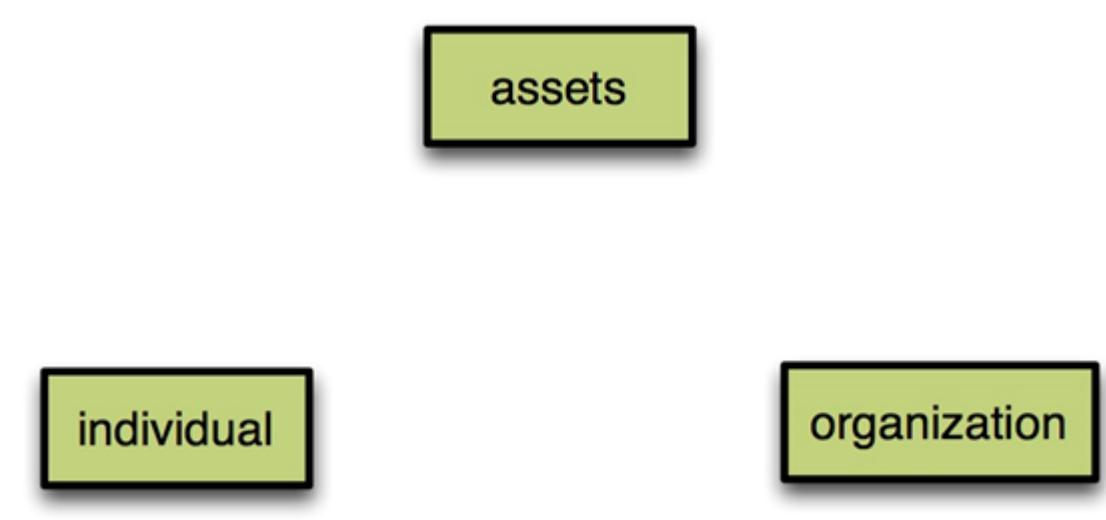
- **Inspired by Travis Breau**
  - *captured state notification laws in DL*
  - Looks like this:
    - *is(insider, anyone(authorized to use(computers and networks)))*
    - *is(insider, anyone(operating inside (security perimeter)))*



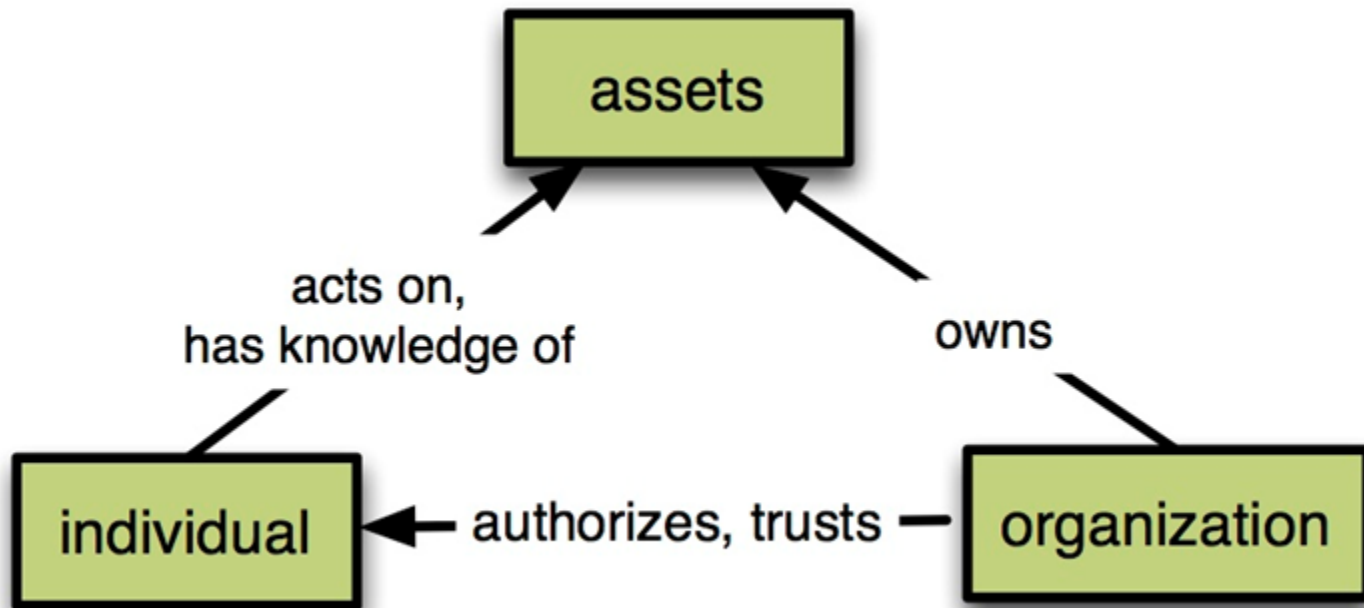
Software Engineering Institute

Carnegie Mellon

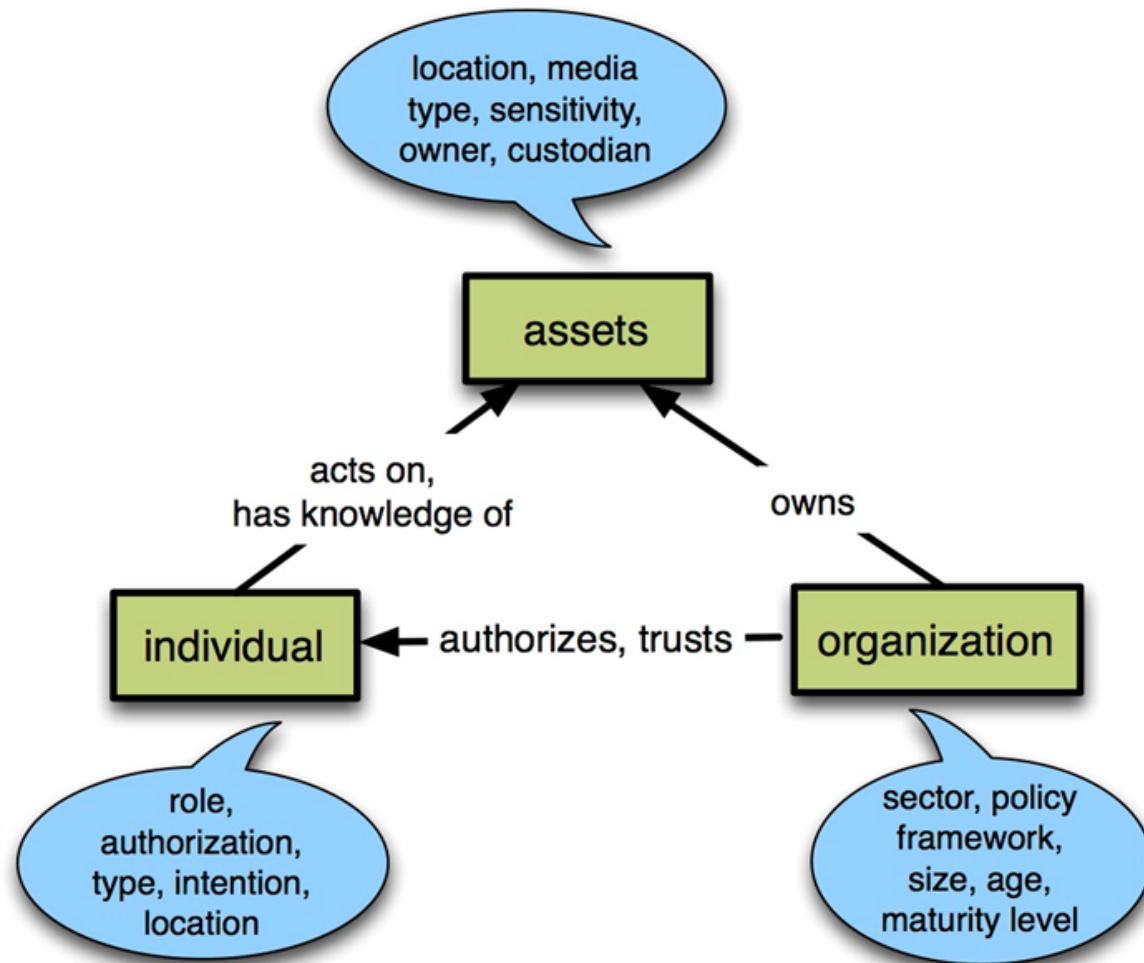
# From Formal Language to Structure



# From Formal Language to Structure



# From Formal Language to Structure



# Draft Ontology



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# An Ontology for Insider Threat Indicators



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# Design Goals

- Goal # 1: Focus on detection
  - Goal # 2: Make indicator definition simple
  - Goal # 3: Be agnostic and compatible with existing models
  - Goal # 4: Be easily extensible
- 
- Assumption #1: The focus should be on the person
  - Assumption #2: Indicators should target significant events



Software Engineering Institute

CarnegieMellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# The Ontology in OWL





# A Sample Indicator

Indicators use simple subject-verb-object (SVO) syntax borrowed from natural language.

**if** entity:securityRoleEntity:systemAdministrator  
**performs** action:dataMovementAction:egress:printing  
**on** object:dataObject:anyDataObject  
**within** time:definedScheduleTime:non-work-hours  
**perform** analysis:binaryAnalysis



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# A Sample Indicator

Indicators use simple subject-verb-object (SVO) syntax borrowed from natural language.

if systemAdministrator  
performs printing  
on anyDataObject  
within non-work-hours  
perform binaryAnalysis



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University



# CERT's Insider Threat Services



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# Insider Threat Assessment (ITA)

**Objective:** To measure an organization's level of preparedness to address insider threats to their organization.

**Method:** Document Review, Process Observation, and Onsite interviews using insider threat assessment workbooks based on all insider threat cases in the CERT case library.

**Outcome:** Confidential report of findings with findings and recommendations.

**Areas of Focus:** Information Technology/Security; Software Engineering; Data Owners; Human Resources; Physical Security; Legal / Contracting; Trusted Business Partners.



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# CERT Insider Threat Workshops

**Goal:** participants leave with actionable steps they can take to better manage the risk of insider threat in their organization

½ day, One day, Two days - Presentations and interactive exercises

Addresses technical, organizational, personnel, security, and process issues

## Exercises

- Address portions of the insider threat assessment
- Purpose: assist participants in assessing their own organization's vulnerability to insider threat in specific areas of concern



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# Building an Insider Threat Program

**Goal:** CERT staff work with senior executives from across the organization to develop a strategic action plan, based on actual cases of insider threats at the participating organization and research by CERT staff, to address and mitigate the risk of insider threat at the organization.

- Key differences from standard workshop
  - Tailored course material based on actual insider incidents at the organization.
    - Cases are provided in advance by the organization, and treated with strict confidentiality.
    - Workshop is preceded by a 3-day onsite by CERT staff to work with the organization's staff to familiarize themselves with the provided case material.
  - Second day of workshop CERT staff and executives work together to create the Organization's strategic plan for preventing, detecting and responding to insider threats.



Software Engineering Institute

CarnegieMellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [#CERTinsiderthreat](#)  
© 2013 Carnegie Mellon University

# CERT Resources

Insider Threat Center website  
([http://www.cert.org/insider\\_threat/](http://www.cert.org/insider_threat/))

Common Sense Guide to Mitigating Insider Threats, 4th Ed.  
(<http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm>)

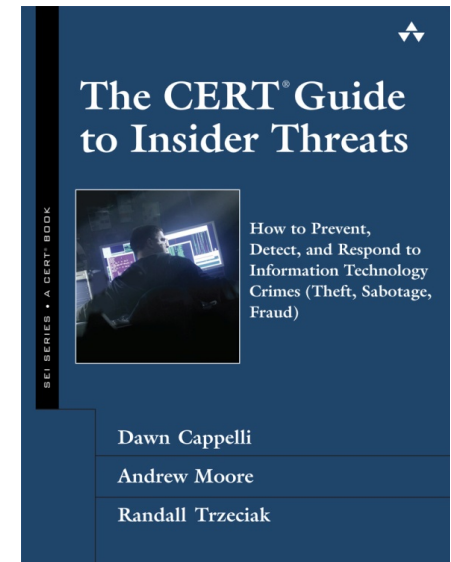
Insider threat workshops

Insider threat assessments

New controls from CERT Insider Threat Lab

Insider threat exercises

[The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes \(Theft, Sabotage, Fraud\) \(SEI Series in Software Engineering\)](#) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak



Software Engineering Institute

Carnegie Mellon

Managing The Insider Threat:  
What Every Organization Should Know  
Twitter [\*\*#CERTinsiderthreat\*\*](#)  
© 2013 Carnegie Mellon University

Copyright 2013 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of AFCEA or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM-0000550



**Software Engineering Institute**

**CarnegieMellon**

Managing The Insider Threat:  
What Every Organization Should Know  
**Twitter #CERTinsiderthreat**  
© 2013 Carnegie Mellon University